JA998173

#4

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed this Office.

出願年月日
Date of Application: １９９８年１２月２８日

出願番号
Application Number: 平成１０年特許願第３７２３５５号

出願人
Applicant (s): インターナショナル・ビジネス・マシーンズ・コーポレイション

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９９年 ７月１３日

特許庁長官
Commissioner,
Patent Office 伴佐山建志

【書類名】　特許願

【整理番号】　JA998173

【提出日】　平成10年12月28日

【あて先】　特許庁長官　伊佐山　建志　殿

【国際特許分類】　H04N　7/18

【発明の名称】　デジタルデータ認証システム

【請求項の数】　9

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　上條　浩一

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　森本　典繁

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　小出　昭夫

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　阪倉　　徹

【特許出願人】

【識別番号】　390009531

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレイション

【氏名又は名称原語表記】　INTERNATIONAL BUSINESS MACHINES CORPORATION

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【弁理士】

【氏名又は名称】　市位　嘉宏

【復代理人】

【識別番号】　100059258

【弁理士】

【氏名又は名称】　杉村　暁秀

【復代理人】

【識別番号】　100072051

【弁理士】

【氏名又は名称】　杉村　興作

【復代理人】

【識別番号】　100098383

【弁理士】

【氏名又は名称】　杉村　純子

【手数料の表示】

【予納台帳番号】　015093

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9304391

【包括委任状番号】　9304392

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　デジタルデータ認証システム

【特許請求の範囲】

【請求項１】　入力装置から入力されたデジタルデータをメモリ装置へ書き込むとともに、書き込まれたメモリ装置内のデジタルデータを受信装置へ転送するシステムにおいて、

（１）入力装置からメモリ装置へのデジタルデータの書き込みおよびメモリ装置から受信装置へのデジタルデータの転送をする際に、入力装置とメモリ装置との間およびメモリ装置と受信装置との間それぞれで機器の認証を行い、

（２）メモリ装置にデジタルデータを書き込む際、デジタルデータに一方向ハッシュ関数による電子署名を施すとともに、メモリ装置からデジタルデータを読み出して転送する際、施した電子署名を解読して、デジタルデータが記録時から改変がないことを確認した後転送する、

ことを特徴とするデジタルデータ認証システム。

【請求項２】　前記入力装置からメモリ装置へ書き込むべきデジタルデータ、および、メモリ装置から受信装置へ転送すべきデジタルデータに、機器認証データを織り交ぜる請求項１記載のデジタルデータ認証システム。

【請求項３】　前記入力装置および受信装置との認証、および、前記メモリ装置内でのデジタルデータへの認証および施した認証の解読を、メモリ装置に内蔵したＣＰＵにより行う請求項１または２記載のデジタルデータ認証システム。

【請求項４】　前記入力装置とメモリ装置との間、および、メモリ装置と受信装置との間の認証が成功した場合のみ、前記入力装置からメモリ装置へのデジタルデータの書き込みおよび前記メモリ装置から受信装置へのデジタルデータの転送を行い、認証が成功しなかった場合は、通常のデジタルデータの書き込みおよび転送を行う請求項１～３のいずれか１項に記載のデジタルデータ認証システム。

【請求項５】　前記入力装置とメモリ装置との間では、両者の認証のために使用する特定の共通の暗号化関数Ｈｄｃと内部鍵Ｋｄｃを持ち、前記メモリ装置は、メモリ装置内の電子署名に使用するハッシュ関数Ｈｃｆと内部鍵Ｋｃｆを持ち、前記メモリ装置と入力装置との間では、両者の認証のために使用される特定の共

通の暗号化関数Ｈｐｃとその鍵Ｋｐｃを持つ請求項１～４のいずれか１項に記載のデジタルデータ認証システム。

【請求項６】　前記関数Ｈｄｃ、Ｈｃｆ、Ｈｐｃおよびそれらの鍵Ｋｄｃ、Ｋｃｆ、Ｋｐｃが、それぞれの装置のＲＯＭに格納されている請求項５記載のデジタルデータ認証システム。

【請求項７】　前記関数Ｈｐｃが暗号化されてＲＯＭに格納される請求項６記載のデジタルデータ認証システム。

【請求項８】　前記入力装置からメモリ装置への認証を公開鍵方式を利用して行う請求項１～７のいずれか１項に記載のデジタルデータ記録システム。

【請求項９】　前記メモリ装置がコンパクトフラッシュであり、前記ハッシュ関数によるデジタルデータの電子署名を、記録領域における各ページのＥＣＣの計算の対象とならない冗長エリアに記憶する請求項１～８のいずれか１項に記載のデジタルデータ記録システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタルカメラなどのデジタルデータ入力装置からデータの一時保管メモリを経由して転送されるデジタルデータの保全、つまり改ざんや改変防止のためのデジタルデータ記録システムに関するもので、特に、デジタルカメラによって撮影された損害保険の査定用デジタル写真や、建設現場における作業記録用のデジタル写真の改変防止をすることのできるシステムに関するものである。

【０００２】

【従来の技術】

近年、デジタルカメラなど民生用デジタル機器の急速な普及により、多くの分野でデジタルデータの利用が進んでいる。しかし、デジタルデータは、痕跡を残さずにコンテンツを改変される危険性があるので、証拠として使うにはリスクを伴う。データの受け取り手が、データを信用するためには、データが取得されてから改変が無いことを保証する手段が必要となる。

【０００３】

デジタル・データの改ざんや改変を防ぐ方法としては、ＭＡＣ（Message Authentication Coding ）など一方向ハッシュ関数によって作成した電子署名をデータに添付して転送する方法がある。デジタル画像の場合は、この電子署名を画像無いに電子透かしを使用して埋込画像との一体性をさらに高めることもできる（例えば、特開平１０－１６４５４９号公報）。

【０００４】

【発明が解決しようとする課題】

しかし、この技術が最も必要とされるデジタル写真への適用を考慮した場合、電子署名を施すのはカメラの中になる。その場合、カメラ側にかかる計算負荷が大きい上に、カメラ内に保管される暗号鍵は固定となるので、より信頼性の高いシステムが望まれる。つまり、現在の機器のハード的な制約の範囲内で実現可能で、かつ、必要十分なデータの保全性を確保できる方法が必要となっていた。

【０００５】

本発明の目的は上述した課題を解消して、データ自体に秘密性はないが改善や差し替えによるデータの改変やなりすましを防止し、データを保全することができるデジタルデータ認証システムを提供しようとするものである。

【０００６】

【課題を解決するための手段】

本発明は、入力装置から入力されたデジタルデータをメモリ装置へ書き込むとともに、書き込まれたメモリ装置内のデジタルデータを受信装置へ転送するシステムが対象となる。このシステムにおいて、まず、入力装置からメモリ装置へのデジタルデータの書き込みおよびメモリ装置から受信装置へのデジタルデータの転送をする際に、入力装置とメモリ装置との間およびメモリ装置と受信装置との間それぞれで機器の認証を行う。同時に、メモリ装置にデジタルデータを書き込む際、デジタルデータに一方向ハッシュ関数による電子署名を施すとともに、メモリ装置からデジタルデータを読み出して転送する際、施した電子署名を解読して、デジタルデータが記録時から改変がないことを確認した後転送する。

【０００７】

本発明では、まず、デジタルデータの入力装置からメモリ装置へのデータの書

き込み、および、メモリ装置から受信装置へのデータの転送をする際に、それぞれの機器の認証を行うことで、デジタルデータの入力装置からメモリ装置を介して受信装置へのデータ転送経路を限定することができる。また、メモリ装置にデータを記録する際、好ましくは内蔵のＣＰＵによりデータを一方向ハッシュ関数により電子署名を施すことで、メモリ装置への直接アクセスによるデータの改変を防止することができる。これにより、データ自体に秘密性はないが改善や差し替えによるデータの改変やなりすましを防止し、データを保全することができる。

【０００８】

【発明の実施の形態】

図１は本発明のデジタルデータ認証システムの一例を説明するための図である。図１に示す例において、入力装置１００はデジタルカメラ、メモリ装置２００はコンパクトフラッシュ、受信装置３００は画像データを管理するパーソナルコンピュータとした。メモリ装置２００は着脱式に限定せず、カメラ内蔵のメモリでも同様である。なお、以下の説明において、「通常のデータ転送」というのは、認証を伴わない指定されていない装置との間でも正しく動作するデータ転送のことをいう。また、本発明に係る認証機能を持ったデジタルカメラをＳＤＣ（Secured Digital Camera）と、本発明に係る認証機能を持ったメモリ装置をＳＣＦ（Secured Compact Flash ）と、本発明に係る認証機能を持ったパーソナルコンピュータをＳＰＣ（Secured Personal Computer ）とする。さらに、ＤＣ、ＣＦ、ＰＣは各々一般のデジタルカメラ、コンパクトフラッシュ、パーソナルコンピュータを示すものとする。

【０００９】

まず、本発明のデジタルデータ認証システムを実行するにあたっての前提条件を説明する。始めに、特定された入力装置１００、メモリ装置２００および受信装置３００の間では、特定の共通なコマンド（Request SeedコマンドとSend Seed コマンド）を定義する。一般の装置はこれらのコマンドに対し、エラーを返すかタイムアウトになる。Request Seedコマンドは、クライアントにシードを投げる事を要求するコマンドで、Send Seed コマンドは、クライアントにこれからシ

ードを投げる事を知らせるコマンドである。次に、特定された入力装置（ＳＤＣ）１００とメモリ装置（ＳＣＦ）２００の間では、特定の暗号化関数Ｈｄｃとその鍵Ｋｄｃを持っている。また、メモリ装置２００はあるハッシュ関数Ｈｃｆと内部鍵Ｋｃｆを持っている。これらはそれぞれの装置のＲＯＭに格納されており、装置の外部に漏れる事はない。但し、この場合関数Ｈｄｃ、Ｈｃｆは外部に漏れても機密性は保たれる。

【００１０】

次に、特定されたメモリ装置（ＳＣＦ）２００と受信装置（ＳＰＣ）３００との間では、特定の共通の暗号化関数Ｈｐｃとその鍵Ｋｐｃを持っている。メモリ装置２００においてＫｐｃはＮＡＮＤ記録空間２１０に格納されているが、Ｋｐｃはある暗号化関数Ｅｘとその鍵Ｋｘに因って暗号化されて格納されている。Ｈｐｃ、Ｅｘ、Ｋｘはそれぞれの装置のＲＯＭに格納されている。受信装置３００でもＫｐｃはある暗号化関数Ｅ２ｐｃとその鍵パスワードに因って暗号化されている。パスワードはＳＣＦの所有者のアクセスできないところに格納されているか、それ自体暗号化されている。その詳細は後述する。以下、図１を参照して各プロセスにおける各装置の機能を説明する。

【００１１】

（１）デジタル画像のメモリ装置への記録について：

図１において、画像の取り込み部１１０で取得された画像は、画像処理部１２０を経由してメモリ装置２００のＮＡＮＤ記録空間２１０に記録される。メモリ装置２００は、入力装置１００からのデータ書き込み要求がきた際、メモリ装置２００の相互認証部２３１が内蔵のＣＰＵ２２０経由で入力装置１００の相互認証部１３０に対して装置認証を行う。認証が成功した場合のみ画像処理部１２０からＮＡＮＤ記録空間２１０へのデータ記録が実行される。この認証は、セキュリティレベルを増すために、また、装置認証成功後に装置のすり替えができないように、データ転送の続く間も断続的に繰り返すよう構成することもできる。その内容については後述する。以下、実際の処理プロセスを説明する。

【００１２】

（１．１）ＳＤＣはＣＦに対してRequest Seedコマンドを投げ、ある乱数（＝Ｒ

１）を要求する。この際、エラーが返ってくるか応答がない場合、ＳＤＣはＣＦがＳＣＦでないと判断し、通常のデータ転送を行う。

（１．２）ＳＣＦはＲ１をＳＤＣに返す。シードを要求される前に通常のライトコマンドが来た場合、ＳＣＦはＤＣがＳＤＣでないと判断し、通常のデータ転送を行う。

（１．３）ＳＤＣはデータ転送を始める。ＣＦは通常、１回のライトコマンドで１ページ（＝５１２バイト）のデータ転送を最大２５６回繰り返す。

（１．４）ＳＤＣは（１．２）でＲ１がＣＦから返ってきた場合、Ｒ１を鍵Ｋｄｃを使って暗号化したＲ＿Ｅｄを以下の式（１）で計算し、ＣＦに返す。ＫｄｃはＳＤＣとＳＣＦ間の秘密鍵である。

Ｒ＿Ｅｄ＝Ｈｄｃ（Ｋｄｃ，Ｒ１）　　‥‥（１）

（１．５）ＳＣＦは自分の持っているＨｄｃとＫｄｃ、ＤＣに送ったＲ１を使って上記式（１）の計算を行い、Ｒ＿ＥｄがＤＣから来たものと一致するかどうか確認する。Ｒ＿Ｅｄが一致しなかった場合、ＤＣはＳＤＣでないと判断し、そのページも含め、今回のライトコマンドに対するデータ転送は、通常のデータ転送を行う。

【００１３】

（２）メモリ装置内のデータ保護について：

上記（１．５）でＲ＿Ｅｄが一致した場合、ＳＣＦは更に、その次の認証が行われるまでの間に受け取りページに対して記録する画像に、ＣＰＵで生成した認証マーク（フラグ）を付加して電子署名を行い、ＮＡＮＤ記録空間２１０に記録する。認証がない場合には認証マークを付加せずに記録する。ＣＦは１ページに付き１６バイトのＥＣＣの計算の対象とならない冗長エリアを有し、その内４バイトはリザーブドエリアのため、そのエリアに上記フラグを書くことができる。コンパクトフラッシュの詳細な構成については後述する。認証マークは送られてくるデータのハッシュを取ることで求めるが、データの全てに対してハッシュをとるとコストがかかる場合、ハッシュをかけるべきデータも暗号で決めれば良い。この際、データ全体でハッシュをとらない事によるセキュリティが心配されるが、通常、ＤＣからのデータはＪＰＥＧで圧縮されており、部分（例えば１バイ

ト）単位のスワップではデータ自体を改変するのは非常に困難なため、セキュリティは十分保たれると考えられる。ここで、ハッシュの計算には、ＳＣＦのＲＯＭに内蔵された各ＳＣＦにユニークな鍵であるＫｃｆを使う。Ｋｃｆさえ秘密であれば、ハッシュ関数Ｈｃｆ自体は秘密である必要はない。

【００１４】

メモリ装置２００は、データを受信装置３００に転送する際に、内蔵のＣＰＵによりデータの認証アルゴリズムＨｃｆと非公開鍵Ｋｃｆを利用して画像に付された電子署名を解読し、画像が記録時から改変のないことを確認した後、後述するＳＣＦとＰＣ間の認証に対し、正しい答えを返す。改変が検出された場合、ＳＣＦとＰＣ間の認証に対しエラーを返す。

【００１５】

（３）メモリ装置から受信装置へのデータ転送について：

メモリ装置２００のＮＡＮＤ記録空間２１０に記録されているデータは、受信装置３００の記録空間３１０に転送される。この際、メモリ装置２００の相互認証部２３２と受信装置３００の相互認証部３２０との間で機器の認証が行われ、認証が成功した場合のみ、ＮＡＮＤ記録空間２１０から記録空間３１０へのデータ転送が実行される。受信装置３００は、メモリ装置２００からデータを読み出す際に、メモリ装置２００の相互認証部２３２に対して両者で共通の暗号化関数Ｈｐｃと受信装置３００が指定する非公開の鍵Ｋｐｃをもとに認証を行い、正規の受信装置３００であることを確認する。また、上述したように、メモリ装置２００は、データを受信装置３００に転送する際に、内蔵のＣＰＵによりデータの認証アルゴリズムＨｃｆと非公開の秘密鍵Ｋｃｆで画像が記録時からの改変のないことを確認した後、確認済みであることを示すデータを受信装置３００へ伝達する。メモリ装置２００の認証とメモリ装置２００から伝達される「改変なし確認」の情報を拠り所に当該データが所定の入力装置１００から限定された経路を通ってきたデータであることを確認することができる。以下、具体的なプロセスを示す。

【００１６】

（３．１）ＳＰＣはＣＦに対してSend Seed コマンドを投げ、ある乱数（＝Ｒ２

）を投げる事を知らせる。

（３．２）ＳＰＣはＲ２をＣＦに返す。

（３．３）ＳＰＣはデータを読み始めるが、ＣＦは通常１回のリードコマンドで１ページ（＝５１２バイト）のデータ転送を最大２５６回繰り返す。

（３．４）ＳＣＦは先ず、ＰＣが読もうとしているデータにフラグが正しくついているかをＨｃｆとＫｃｆを使い確かめる。正しくない場合は、データは指定されずと判断して、今回のリードコマンドに対する認証に対してはエラーを返す。

（３．５）ＳＣＦは、フラグが正しい場合、送られてきたＲ２に対し、以下の式（２）の計算を行い、Ｒ＿ＥｐをＰＣに返す。ＫｐｃはＳＣＦとＳＰＣとの間の秘密鍵である。

Ｒ＿Ｅｐ＝Ｈｐｃ（Ｋｐｃ，Ｒ２）　　‥‥（２）

（３．６）ＳＰＣは自分の持っているＨｐｃとＫｐｃ、ＣＦに送ったＲ２を使って上記（２）式の計算を行い、計算したＲ＿ＥｐがＳＣＦから来たものと一致するかどうか確認する。もし、一致しなかった場合、ＣＦもしくはリードしようとしているデータは指定したものでないと判断する。

（３．７）ＳＰＣは、Ｒ＿Ｅｐの計算結果がＣＦから来たものと一致した場合、対象のリードデータに対して、全てリードし終わるまでリードコマンドを送る毎に最低１回はシードを送り認証をし、全てのページに対して認証が正しく行われた場合のみそのデータはＳＤＣから改ざん無しでＳＣＦ経由で来たものと判断する。この一連の動作により、ＳＰＣは、受け取ったデータの入力元と改ざんの有無を確認する事が出来る。図２に上述したＳＤＣからＳＣＦを介してＳＰＣへの認証およびデータの流れの概念を示す。

【００１７】

次に、上述した本発明のデジタルデータ認証システムにおいて好適に使用できるコンパクトフラッシュの構造について説明する。コンパクトフラッシュは、１９９４年サンディスクより発表された小型不揮発性メモリで、ＰＣＭＣＩＡ－ＡＴＡコンパチブルで電気的、メカ的にＴｙｐｅIIのＰＣＭＣＩＡカードとして使用することが出来る。容量としては、４Ｍ、８Ｍ、１６Ｍバイト等があり、デジタルカメラで撮られたＪＰＥＧイメージ（５０ｋから１００ｋバイト）の記憶な

ど幅広い用途がある。コンパクトフラッシュの大きな特徴は、小型で大容量でありながらＣＰＵを内蔵している点にある。図３にコンパクトフラッシュの内部構造の一例を、図４に物理フォーマット仕様（８Ｍバイト）の一例を、図５にページモデルの一例を、それぞれ示す。本発明では、図５に示す冗長領域のReserved Area にフラグを書き込んでいる。

【００１８】

以上で、本発明のデジタルデータ認証システムの主要な部分の説明が終了した。次に、その他の運用上の選択肢について、公開鍵による運用と認証セクターのマルチプレクスとＰＣにおけるＫｐｃの暗号化の一例について説明する。まず、

（４）公開鍵による運用について：

ＳＤＣとＳＣＦの間の認証機構において、公開鍵方式を利用することにより、カメラの「なりすまし」による改ざん画像のＳＣＦへの書き込みをより困難にすることができる。これは、カメラ側にチャレンジ用のデータを暗号化する秘密鍵、ＳＣＦ側にカメラからの回答を認証するための公開鍵を持たせることで達成することができる。

【００１９】

（５）認証セクターのマルチプレクスについて：

装置の認証は、主体となる装置（ＳＤＣとＳＣＦの場合はＳＣＦ、ＳＣＦとＳＰＣの場合はＳＰＣ）が相手側の装置にチャレンジ用のデータを送り、所定の暗号化によって変換され、返送されてくるデータを手元の暗号によって確認することで完結する。装置の認証プロセスとその後のデータ転送が独立している場合には、認証の完了を見計らって別の入力装置につなぎかえることによって、装置の「なりすまし」ができる危険性がある。これを防ぐために、入力装置からは継続的に認証データを、転送データに織り交ぜて送るようにした。認証データを織り交ぜるルールは、チャレンジデータを暗号化したあとの回答（Ｒ＿Ｅｄ、Ｒ＿Ｅｐ）から生成するものとし、直接な認証データの転送と、そのデータを転送するルールの双方で相手方の装置の認証を行う。

【００２０】

（６）ＰＣにおけるＫｐｃの暗号化の一例について：

まず、本構成における限定条件は以下の通りである。

１．ＳＤＣ、ＳＣＦ内のＲＯＭの中身に対する攻撃に対しては、ＲＯＭのコードは外からは解析出来ず、ＲＯＭを分解しても中身の解析は出来ないtaper resistである。因って、この中に入っている鍵（Ｋｄｃ、Ｋｐｃ、Ｋｃｆ、Ｋｘ）も攻撃することができない。

２．ＳＰＣにおけるアップロード用の暗号鍵ＫｐｃはＳＰＣの管理者が管理していて、且つ、暗号化されているため、ＳＣＦの所有者には推測不可能である。万が一ＳＣＦの所有者がＰＣのアップロードプログラムを解読し、そのＰＣ内のＫｐｃを推測する可能性がある場合、以下の対策を講じることができる。

【００２１】

（ａ）Ｋｐｃのインストール時

ＰＣの管理者はＫｐｃのインストール時に以下の式（３）によりＫｐｃを暗号化したＫｐｃ’を計算し、ＰＣに記憶する。

Ｋｐｃ’＝Ｅ２ｐｃ（パスワード，Ｋｐｃ）　　・・・・（３）

ここで、Ｅ２ｐｃはＫｐｃを暗号化するための暗号化関数で、パスワードはＰＣ管理者のみが知り得るパスワードである、また、パスワードを以下の式（４）によりハッシュしたパスワード’もＰＣに記憶する。この際、パスワード自体は記憶しない。

パスワード’＝Ｈｐａｓｗ（パスワード）　　・・・・（４）

ここで、Ｈｐａｓｗは一方向ハッシュ関数である。

【００２２】

（ｂ）ＳＣＦとＳＰＣとの間の認証時

ＳＰＣの管理者はパスワードを入力する。ＳＰＣのアップロードプログラムは入力されたパスワードより（４）式を計算し、計算値が記憶されているパスワード’と一致した場合、以下の式（５）よりＫｐｃを計算し、認証に使用する。

Ｋｐｃ＝Ｄ２ｐｃ（パスワード，Ｋｐｃ’）　　・・・・（５）

ここで、Ｄ２ｐｃはＥ２ｐｃに対する復号化関数で、任意の値ｘ、ｙに対し、以下の式（６）が成立する。

ｘ＝Ｄ２ｐｃ（ｙ，Ｅ２ｐｃ（ｙ，ｘ））　　・・・・（６）

この方法により、悪意のある者がＰＣよりＫｐｃ’、パスワード’、Ｅ２ｐｃ、Ｄ２ｐｃ、Ｈｐａｓｗを見つけ出す事に成功しても、そこからＫｐｃを推測することは不可能である。

【００２３】

上述した本発明の利点を以下にまとめる。

（１）ＳＤＣとＳＣＦとの間、および、ＳＣＦとＳＰＣとの間で、それぞれ機器の認証を行っているため、入力装置から受信装置までのデータ転送経路を限定することができる。

（２）ＳＤＣとＳＣＦとの間、および、ＳＣＦとＳＰＣとの間のデータ転送は、認証セクタをデータにマルチプレクスして、断続的に認証を行うことにより、装置の認証成功後に認証のない入力装置をすりかえることが防止できる。

（３）ＳＣＦのメモリ領域にデータを記録する際に、ＳＣＦのＲＯＭ内の秘密の鍵を使ったハッシュ関数で署名を施すため、ＮＡＮＤ記録空間２１０を分解し、改ざんしたデータに置き換えることを防止することができる。

（４）ＳＤＣ、ＳＰＣとの認証鍵（Ｋｄｃ、Ｋｐｃ）は、ＲＯＭ内の秘密鍵（Ｋｘ）により暗号化されているため、ＳＣＦのＮＡＮＤ記録空間２１０を分解しても盗み出すことはできない。

（５）装置の認証が行われなかったり、失敗した場合でも、データは通常のＣＦと同様にＮＡＮＤ記録空間２１０に記録され、読み出されることができる。ただし、認証がつかない。

（６）本発明のシステムは既存のハードウェアの内蔵プログラムの改造で実現可能なため、カメラメーカへの負担も軽く、デファクト標準として市場に広まることが期待できる。

【００２４】

【発明の効果】

以上の説明から明らかなように、本発明によれば、安価で効果的にデジタルデータの入力装置と受信装置のデータの保全が保証でき、デジタル写真にも証拠能力をもたせることが可能となる。また、本技術の導入には、既存のハードウェアの内蔵プログラムの改造で実現可能なため、カメラメーカの対応への負担も軽く

デファクト標準として市場に広まることが期待できる。また、転送データの安全性の観点からデジタル化を見合わせている企業などのデジタル化を促進することができる。

【図面の簡単な説明】

【図１】　本発明のデジタルデータ認証システムの一例を説明するための図である。

【図２】　本発明における認証およびデータの流れの概念を示す図である。

【図３】　コンパクトフラッシュの内部構造の一例を示す図である。

【図４】　コンパクトフラッシュの物理フォーマットの一例を示す図である。

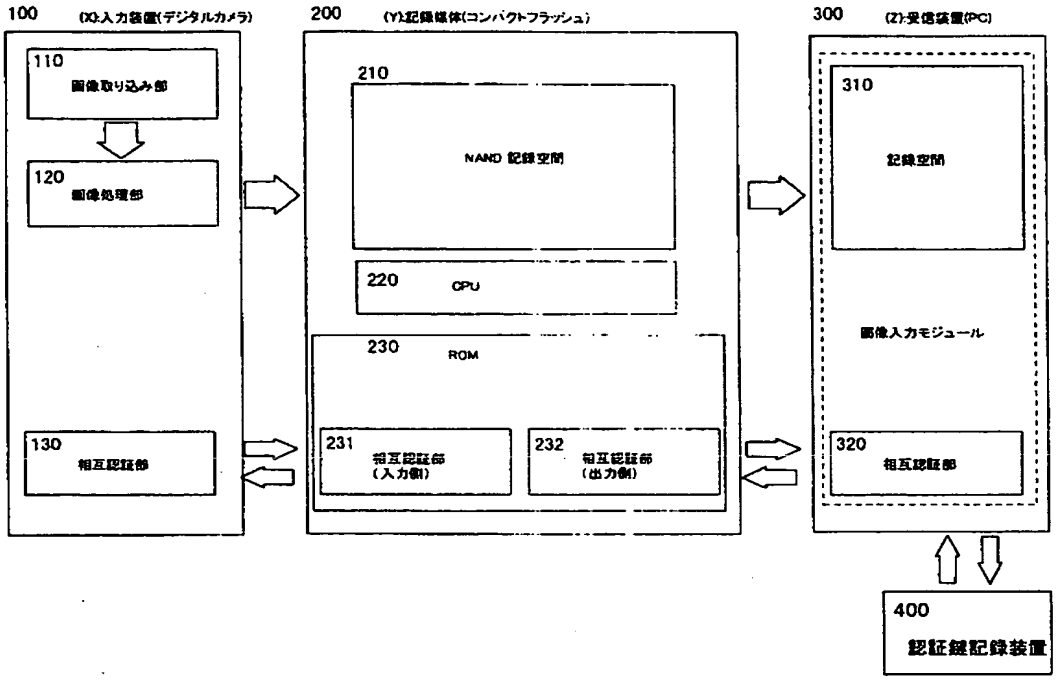
【図５】　コンパクトフラッシュにおけるページモデルを示す図である。

【符号の説明】

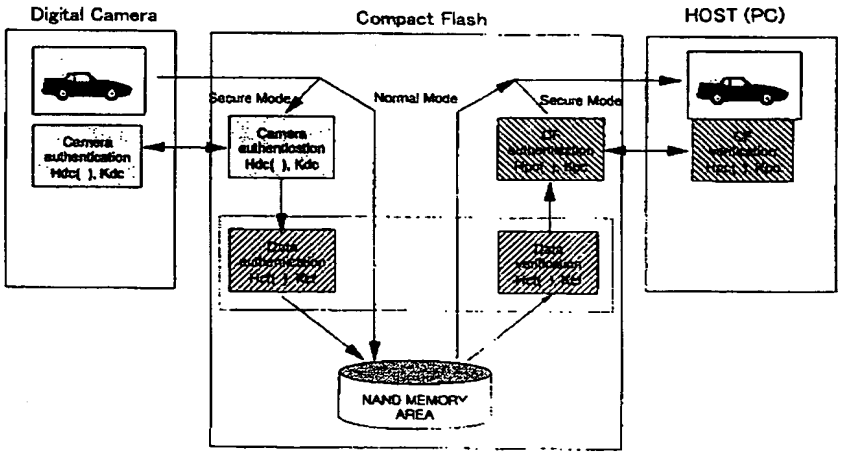
１００　入力装置、１１０　画像取り込み部、１２０　画像処理部、１３０相互認証部、２００　メモリ装置、２１０　ＮＡＮＤ記録空間、２２０　ＣＰＵ、２３０　ＲＯＭ、２３１、２３２　相互認証部、３１０　記録空間、３２０相互記録部

【書類名】　図面

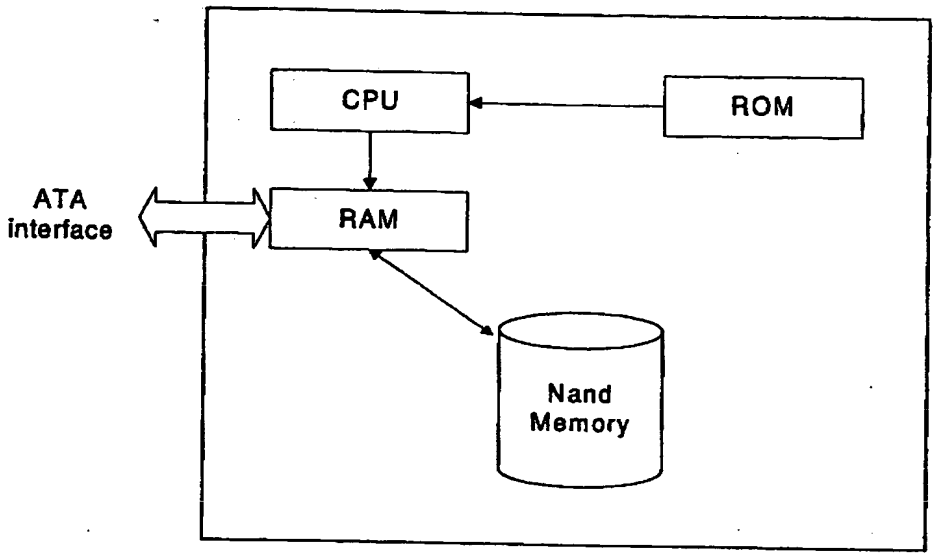
【図１】


100
(X)入力装置(デジタルカメラ)
110
画像取り込み部
120
画像処理部
130
相互認証部
200
(Y)記録媒体(コンパクトフラッシュ)
210
NAND 記録空間
220
CPU
230
ROM
231
相互認証部
(入力側)
232
相互認証部
(出力側)
300
(Z)受信装置(PC)
310
記録空間
画像入力モジュール
320
相互認証部
400
認証鍵記録装置

【図２】


Digital Camera
Compact Flash
HOST (PC)
Secure Mode
Normal Mode
Secure Mode
Camera authentication Hdc( ), Kdc
NAND MEMORY AREA

【図３】



【図４】

		0	511 512	527
Block 0	Page 0	データ領域(512Byte)		冗長部(16Byte)
	Page 1			
	:			
	Page 15			
Block 1	Page 0			
	Page 1			
	:			
	Page 15			
:	:	:		:
:	:	:		:
:	:	:		:
:	:	:		:
:	:	:		:
Block 999	Page 0			
	Page 1			
	:			
	Page 15			

【図５】

◎データ領域（512Byte）

Byte	全ページ
0 ～ 255	Data Area-1
256 ～ 511	Data Area-2

◎冗長領域（16Byte）

Byte	全ページ
512	Reserved Area
513	
514	
515	
516	Data Status Area
517	Block Status Area
518	Block Address Area-1
519	
520	ECC Area-2
521	
522	
523	Block Address Area-2
524	
525	ECC Area-1
526	
527	

【書類名】　　要約書

【要約】

【課題】　データ自体に秘密性はないが改善や差し替えによるデータの改変やなりすましを防止し、データを保全することができるデジタルデータ認証システムを提供する。

【解決手段】　入力装置１００からメモリ装置２００へのデジタルデータの書き込みおよびメモリ装置２００から受信装置３００へのデジタルデータの転送をする際に、入力装置とメモリ装置との間およびメモリ装置と受信装置との間それぞれで機器の認証を行う。同時に、メモリ装置２００にデジタルデータを書き込む際、デジタルデータに一方向ハッシュ関数による電子署名を施すとともに、メモリ装置２００からデジタルデータを読み出して転送する際、施した電子署名を解読して、デジタルデータが記録時から改変がないことを確認した後転送する。これにより、データ自体に秘密性はないが改善や差し替えによるデータの改変やなりすましを防止し、データを保全することができる。

【選択図】　　図１

認定・付加情報

特許出願の番号	平成１０年　特許願　第３７２３５５号
受付番号	５９８００８５４７００
書類名	特許願
担当官	深沢　敏　　２３０７
作成日	平成１１年　２月２２日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 390009531
- 【住所又は居所】 アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
- 【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレイション

【代理人】
- 【識別番号】 100086243
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
- 【氏名又は名称】 坂口　博

【代理人】
- 【識別番号】 100091568
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
- 【氏名又は名称】 市位　嘉宏

【代理人】 申請人
- 【識別番号】 100059258
- 【住所又は居所】 東京都千代田区霞が関３－２－４　霞山ビル７階
- 【氏名又は名称】 杉村　暁秀

【代理人】
- 【識別番号】 100072051
- 【住所又は居所】 東京都千代田区霞が関３－２－４　霞山ビル７階
- 【氏名又は名称】 杉村　興作

【代理人】
- 【識別番号】 100098383
- 【住所又は居所】 東京都千代田区霞が関３丁目２番４号　霞山ビルディング７階　杉村萬國特許事務所内

次頁有

認定・付加情報（続き）

【氏名又は名称】　杉村　純子

次頁無

出　願　人　履　歴　情　報

識別番号　　〔３９０００９５３１〕

１．変更年月日　　１９９０年１０月２４日
［変更理由］　新規登録
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレイション